

REMARKS

Applicants have carefully studied the outstanding Official Action. The present amendment is intended to be fully responsive to all points of rejection and is believed to place the application in condition for allowance. Favorable reconsideration and allowance of the present application are hereby respectfully requested.

Claims 1 – 42 were examined, claims 6 and 23 have been canceled, and thus claims 1 – 5, 7 – 22 and 24 – 42 are now pending in the application.

Claims 1 – 4, 11, 14, 18 – 21, 28, 31 and 35 – 36 stand rejected under 35 USC 103(a) as being obvious over US Patent 6,111,952 to Patarin (hereinafter Patarin) in view of US Patent 5,375,170 to Shamir (hereinafter Shamir).

Claims 5 – 6, 8, 15, 22, 23, 25 and 32 stand rejected under 35 USC 103(a) as being unpatentable over Patarin in view of Shamir as applied to claim 1, and further in view of an article of Shamir et al titled “Cryptanalysis of the Oil and Vinegar Signature Scheme” (hereinafter Shamir2).

Claims 7, 9, 10, 16 - 17, 24, 26 - 27, and 33 - 34 stand rejected under 35 USC 103(a) as being unpatentable over Patarin in view of Shamir as applied to claim 1, and further in view of US Patent 5,790,675 to Patarin (hereinafter Patarin2).

Claims 12 – 13 and 29 – 30 stand rejected under 35 USC 103(a) as being obvious over Patarin in view of Shamir, and further in view of an article of Patarin titled “Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two Families of Asymmetric Algorithms” (hereinafter Patarin3).

Claims 37 – 42 stand rejected under 35 USC 103(a) as being unpatentable over Patarin in view of Shamir and further in view of Applicant’s Admitted Prior Art (hereinafter AAPA) and further in view of Shamir2.

Patarin describes an asymmetric cryptographic communication process which establishes a correspondence between a first value (x) represented by n elements (x_1, \dots, x_n) of a ring (A) and a second value (y) represented by m elements (y_1, \dots, y_m) of this ring, n and m being integers greater than or equal to 2.

Shamir describes a signature scheme based on birational permutations.

Shamir2 describes two algebraic attacks which can efficiently separate the oil and vinegar variables of Patarin's "Oil & Vinegar" scheme.

Patarin2 describes an asymmetrical cryptographic scheme which can be used for enciphering.

Patarin3 describes two new families of asymmetric algorithms: Hidden Field Equations (HFE); and Isomorphisms of Polynomials (IP).

In rejecting claim 1 the Examiner takes the position that Patarin discloses all the features of claim 1 except the features of providing a message to be signed, applying a hash function on the message to produce a series of k values b_1, \dots, b_k , and applying the secret key operation to transform a'_1, \dots, a'_{n+v} to a digital signature e_1, \dots, e_{n+v} , and that the features that are not present in Patarin are disclosed in Shamir.

Applicants respectfully disagree for the following reasons. The set of equations S1 has two types of variables: x variables; and y variables. The x variables are the variables in which the signature values are substituted, and the y variables are the variables in which the values obtained from hashing the message are substituted. The set of equations S1 is obtained from a set of equations S2 having another set of variables a_1, \dots, a_{n+v} that replaces the set x_1, \dots, x_{n+v} in S1. The variables a_1, \dots, a_{n+v} can be divided into two groups: the first group includes n variables which are the "oil" variables, and the second group includes the remaining v variables which are the "vinegar" variables. Patarin however, does not show or suggest such a separation of variables into two distinct groups.

Additionally, in claim 1 in order to solve the set of equations S1, values for the "vinegar" variables are selected and only then a solvable set of equations with the "oil" variables is obtained. However, Patarin uses another technique that enables solving the set of equations as a whole by hiding in the polynomial equations a specific mathematical structure derived from a different mathematical field, that is, extension fields of finite fields.

Nevertheless, in order to facilitate allowance of the application and make the difference between claim 1 of the present application and Patarin

particularly clear, claim 1 has been amended to include the recitations of claim 6, and claim 6 has been canceled without prejudice.

In rejecting claim 6 the Examiner refers to page 266 in Shamir2 and takes the position that the recitation regarding a need to modify definition of oil and vinegar domains discloses the feature recited in claim 6 of selecting the number v of “vinegar” variables to be greater than the number n of “oil” variables.

Applicants respectfully submit that the Examiner’s interpretation of Shamir2 is incorrect. The recitation on page 266 in Shamir2 refers in fact to changes between the original and simplified versions of the oil and vinegar signature scheme (see, for example, the first two lines in the first full paragraph on page 266 in Shamir2), where the simplified version of the oil and vinegar signature scheme uses only quadratic terms in the published forms and the original version also refers to linear and constant terms (see, for example, lines 7 – 13 of the first full paragraph on page 266 in Shamir2). The modifications affect only the linear and constant terms (see, for example, lines 7 – 8 of the first full paragraph on page 266 in Shamir2). Thus, the modifications of the definition of the oil and vinegar domains have nothing to do with the feature of selecting the number v of “vinegar” variables to be greater than the number n of “oil” variables. Shamir2 therefore does not show or suggest the feature of selecting the number v of “vinegar” variables to be greater than the number n of “oil” variables.

Additionally, Applicants respectfully submit that combining Shamir2 with Patarin and Shamir is improper and would have not resulted in the combination recited in amended claim 1. Specifically, a person skilled in the art is not expected to combine Patarin with Shamir2 because Patarin and Shamir2 use different algebraic structures. Shamir2 deals with quadratic terms which hide a mixture of a linear subspace of the “vinegar” variables and a linear subspace of the “oil” variables, whereas Patarin hides an algebraic structure derived from a univariate polynomial over a large extension ring.

Furthermore, even if a person skilled in the art would have attempted to combine Shamir2 with Patarin and Shamir, such an attempt would have not been successful because neither Patarin nor Shamir2 teaches how to fix the weaknesses of

the original Oil & Vinegar signature scheme. On the contrary, a person skilled in the art referring to the attacking methods described in Shamir2 is likely to assume that the concept of mixing two disjoint sets of variables as in the original Oil & Vinegar signature scheme is a weak cryptographic construction that should be avoided.

Applicants therefore respectfully point out that the Examiner has failed to make a *prima facie* case for the unpatentability of claim 6, and hence of amended claim 1.

Amended claim 1 is therefore deemed allowable.

Claims 2 – 5 and 7 – 14 depend directly or indirectly from claim 1 and recite additional patentable subject matter.

Claims 2 – 5 and 7 – 14 are therefore deemed allowable.

Claim 15 has been rejected on the same basis as claim 6. Thus, the arguments mentioned above with respect to amended claim 1 also apply to claim 15.

Claim 15 is therefore deemed allowable.

Claims 16 and 17 depend from claim 15 and recite additional patentable subject matter.

Claims 16 and 17 are therefore deemed allowable.

Claim 18 has been amended to include the recitations of claim 23, and claim 23 has been canceled without prejudice. Claim 23 has been rejected on the same basis as claim 6. Thus, the arguments mentioned above with respect to amended claim 1 also apply to amended claim 18.

Claim 18 is therefore deemed allowable.

Claims 19 – 22 and 24 – 31 depend directly or indirectly from claim 18 and recite additional patentable subject matter. Claim 27 has been amended to correct a typographical error. The amendment to claim 27 is not believed to affect patentability thereof.

Claims 19 – 22 and 24 – 31 are therefore deemed allowable.

Claim 32 is apparatus claim corresponding to claim 15. The arguments mentioned above with respect to claim 15 also apply to claim 32.

Claim 32 is therefore deemed allowable.

Claims 33 and 34 depend from claim 32 and recite additional patentable subject matter. Claim 33 has been amended for clarification. The amendment to claim 33 is not believed to affect patentability thereof.

Claims 33 and 34 are therefore deemed allowable.

Claim 35 has been amended as claim 18 and further for clarification to remove a redundancy in the functions of the set S1. The arguments mentioned above with respect to amended claim 18 also apply to amended claim 35.

Claim 35 is therefore deemed allowable.

Claim 36 is a product-by-process claim and it depends from claim 1. The arguments mentioned above with respect to amended claim 1 also apply to claim 36.

Claim 36 is therefore deemed allowable.

Claims 37 – 39 depend directly or indirectly from claim 1 and recite additional patentable subject matter.

Claims 37 – 39 are therefore deemed allowable.

Claims 40 – 42 depend directly or indirectly from claim 18 and recite additional patentable subject matter.

Claims 40 – 42 are therefore deemed allowable.

Applicants have also carefully studied the other prior art of record including US Patent 6,076,163 to Hoffstein et al (hereinafter Hoffstein), US Patent 5,351,298 to Smith (hereinafter Smith), and Patarin's article "Asymmetric Cryptography with a Hidden Monomial" (hereinafter Patarin4), which were not applied in rejecting the claims of the present application.

Hoffstein describes methods and apparatus for providing secure user identification or digital signatures based on evaluation of constrained polynomials.

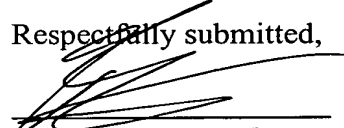
Smith describes a public key cryptographic system that uses Lucas functions as the basis for encoding and decoding messages.

Patarin4 describes a candidate algorithm for asymmetric signatures of length only 64 bits.

Applicants find that Hoffstein, Smith and Patarin⁴ do not affect patentability of the claims of the present application, either when taken separately or in combination with the other prior art of record.

In view of the foregoing amendments and remarks, it is respectfully submitted that the present application is now in condition for allowance. Favorable reconsideration and allowance of the present application are respectfully requested.

Respectfully submitted,



William R. Evans ~~R. Evans~~
c/o Ladas & Parry LLP
26 West 61st Street
New York, New York 10023
Reg. No. 25858
Tel. No. (212) 708-1930